

EXHIBIT C



Records Retention and Protection Policy

Document Ref.	GDPR-DOC-04-1
Version:	1.4
Dated:	11/3/19
Document Author:	Simon Wynn
Document Owner:	Simon Wynn

Records Retention and Protection Policy


Revision History

Version	Date	Revision Author	Summary of Changes
0.9	3/20/18	Simon Wynn	Draft Version
1.0	4/9/18	Simon Wynn	Added HR Info
1.1	5/3/18	Simon Wynn	Updated retention periods
1.2	5/9/18	Simon Wynn	Release version
1.3	5/21/18	Simon Wynn	Formatted for US letter
1.4	1/11/19	Simon Wynn	Annual updates

Distribution

Name	Title
Simon Wynn	SVP, Software Engineering, Head of Privacy
Ameet Patel	Director of Cloud Engineering
William Che	Head of IT
Judi Otteson	General Counsel

Approval

Name	Position	Signature	Date
Simon Wynn	SVP, Software Engineering, Head of Privacy		11/3/19

Records Retention and Protection Policy

Contents

1 INTRODUCTION 3

2 RECORDS RETENTION AND PROTECTION POLICY..... 3

2.1 GENERAL PRINCIPLES 3

2.2 RECORD TYPES AND GUIDELINES 4

2.3 USE OF CRYPTOGRAPHY 7

2.4 MEDIA SELECTION..... 7

2.5 RECORD RETRIEVAL 7

2.6 RECORD DESTRUCTION..... 7

2.7 RECORD REVIEW 8

List of Tables

TABLE 1 – RECORD TYPES AND RETENTION PERIODS 6

1 Introduction

In its everyday business operations Matterport collects and stores records of many types and in a variety of different formats. The relative importance and sensitivity of these records also varies and is subject to the organization's security classification scheme, as documented in the *Matterport Information Security Policy*.

It is important that these records are protected from loss, destruction, falsification, unauthorized access and unauthorized release and a range of controls are used to ensure this, including backups, access control and encryption.

Matterport also has a responsibility to ensure that it complies with all relevant legal, regulatory and contractual requirements in the collection, storage, retrieval and destruction of records. Of particular relevance is the European Union General Data Protection Regulation (GDPR) and its requirements concerning the storage and processing of personal data.

This control applies to all systems, people and processes that constitute the organization's information systems, including employees, suppliers and other third parties who have access to Matterport systems.

The following documents are relevant to this policy:

- *Data Protection Policy*
- *Organization-wide Personal Data Inventory*

2 Records Retention and Protection Policy

This policy begins by establishing the main principles that must be adopted when considering record retention and protection. It then sets out the types of records held by Matterport and their general requirements before discussing record protection, destruction and management.

2.1 General Principles

There are a number of key general principles that must be adopted when considering a record retention and protection policy. These are:

- Records must be held in compliance with all applicable legal, regulatory and contractual requirements
- Records must not be held for any longer than required
- The protection of records in terms of their confidentiality, integrity and availability must be in accordance with their security classification
- Records must remain retrievable in line with business requirements at all times

- Where appropriate, records containing personal data must be subject as soon as possible to techniques that prevent the identification of a living individual

2.2 Record Types and Guidelines

In order to assist with the definition of guidelines for record retention and protection, records held by Matterport are grouped into the categories listed in the table on the following pages. For each of these categories, the required or recommended retention period and allowable storage media are also given, together with a reason for the recommendation or requirement.

Note that these are guidelines only and there may be specific circumstances where records need to be kept for a longer or shorter period of time. This should be decided on a case by case basis as part of the design of the information security elements of new or significantly changed processes and services.

Further information about records held by the organization, including their security classifications and owners can be found in the *Organization-wide Personal Data Inventory*.

Records Retention and Protection Policy

Record Category	Description	Retention Period	Reason for Retention Period	Allowable Storage Media
Accounting	Invoices, purchase orders, accounts and other historical financial records	Minimum of 7 years	IRS and future SOX compliance requirement	Electronic only – paper records must be scanned and stored in Box
Budgeting and Forecasting	Forward-looking financial estimates and plans	Minimum of 7 years	Future SOX compliance requirement	Electronic
System Transaction Logs	Web and app server logs	90 days	Information Security Policy	Electronic
Audit Logs	Security logs e.g. records of logon/logoff and permission changes, API access via AWS Cloud Trail	Minimum of 7 years	Low cost robust storage in AWS enables these to be kept indefinitely	Electronic – AWS S3
Operational Procedures	Records associated with the completion of operational procedures in the form of Jira tickets and Confluence pages	Minimum of 7 years	No business reason to delete records	Electronic
Customer Data	Personal data, including customer names, addresses, order history, but excluding 3D Models/raw scan images	Up to 10 years	Customer may be inactive for a long period of time, but may still require access or make future purchases. IRS and future SOX compliance requirement	Electronic
3D Model data	3D model data, including raw image data and final processed models	Indefinite	Ongoing internal use as defined in the <i>Matterport Cloud Services Agreement</i>	Electronic
Human resources	See document <i>Matterport HR Data Retention Policy</i>			Electronic

Records Retention and Protection Policy

Contractual	Legal contracts, leases	7 years after contract end	Maximum period within which dispute might occur	Electronic only – paper records must be scanned and stored in Box
Employee email and personal computer files	Employee email, local files, files stored in cloud storage and computer profiles	1 year after employee termination	Matterport internal policy	Electronic offline storage (DLT)

Table 1 - Record types and retention periods

2.3 Use of Cryptography

Where appropriate to the classification of information and the storage medium, cryptographic techniques must be used to ensure the confidentiality and integrity of records. Care must be taken to ensure that encryption keys used to encrypt records are securely stored for the life of the relevant records and comply with the organization's policy on cryptography.

Matterport's internal controls require all data at rest be encrypted, regardless of data classification.

2.4 Media Selection

The choice of long term storage media must take into account the physical characteristics of the medium and the length of time it will be in use.

Where records are legally (or practically) required to be stored on paper, adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of paper used. Where possible, backup copies of such records should be taken by methods such as scanning. An approved document storage provider should be used.

For records stored on electronic media such as tape, similar precautions must be taken to ensure the longevity of the materials, including correct storage and copying onto more robust media if necessary. The ability to read the contents of the particular tape (or other similar media) format must be maintained by the keeping of a device capable of processing it.

Records are also stored electronically using cloud storage vendor Box, Google Drive, and in AWS S3.

2.5 Record Retrieval

The choice and maintenance of record storage techniques must ensure that records can be retrieved in a usable format within an acceptable period of time. An appropriate balance should be struck between the cost of storage and the speed of retrieval so that the most likely circumstances are adequately catered for.

2.6 Record Destruction

Once records have reached the end of their life according to the defined policy, they must be securely destroyed in a manner that ensures that they can no longer be used. The destruction procedure must allow for the correct recording of the details of disposal which should be retained as evidence. The *Matterport Information Security Policy* includes detailed data destruction policies and instructions.

2.7 Record Review

The retention and storage of records must be subject to a regular review process carried out under the guidance of management to ensure that:

- The policy on records retention and protection remains valid
- Records are being retained according to the policy
- Records are being securely disposed of when no longer required
- Legal, regulatory and contractual requirements are being fulfilled
- Processes for record retrieval are meeting business requirements